Questions and Answers

About

The Certification and Accreditation of PIV Card Issuing Organizations

1. What is Personal Identity Verification?

Personal Identity Verification (PIV) is the new standard for identification of Federal employees and contractor established in Federal Information Processing Standard (FIPS) 201. Homeland Security Presidential Directive (HSPD) 12 established a policy that such a standard be established and used by all Federal agencies and their contractors to verify the identity of employees seeking access to Federal facilities and information systems. PIV is the method to be used to establish the true identity of a person using identity document authentication techniques and unique biometric characteristics. After establishing the true identity of a current or future Federal employee or contractor, a PIV Card is created and issued to the approved Applicant. The PIV Card is subsequently used as an entry badge to access Federal facilities and as an identity card to access Federal information systems.

2. What is a PIV Card issuing organization?

A PIV Card issuing organization (Issuer) is a Federal organization or a private contractor under the direction and authorization of a Federal agency that is authorized by the head of a Federal Department or Agency to perform the services specified in FIPS 201 for identity proofing and enrolling of approved Applicants (employees, future employees, contractors, guests) in the PIV System and then issuing them new PIV Cards.

3. How many PIV Card Issuing Organizations (Issuers) are expected to exist?

No maximum number of authorized Issuers has been established. One PCI (PCI) per Federal agency is initially expected. However, agencies may cooperate and establish a single PCI for their common needs. Large, geographically distributed agencies may have several PCIs providing PIV services close to where they are needed.

4. What is certification and accreditation?

Certification in this context means a formal process of assessing the attributes (e.g., organization structure, policies, personnel, capabilities, facilities, availability) using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion that a PIV Card issuing organization is reliable and capable of identity proofing and enrolling approved Applicants and issuing PIV Cards in accordance with FIPS 201. Accreditation is granting approval to that organization to perform identity “proofing” and to issue PIV cards to Federal and contractor employee Applicants.

5. Why is accreditation necessary or desirable?

Accreditation is desirable both to Federal agencies and PIV System users by establishing a high level of confidence that: 1) all authorized PCIs have undergone formal capability and reliability assessments; 2) Issuers exhibit appropriate competence and equivalence in their PIV Card issuing processes; and 3) an agency can trust a PIV Card issued by another agency before granting requested accesses based on that verified identity. HSPD 12 recognized the importance of accreditation by requiring that the reliability of all PCIs be accredited before they are authorized to issue PIV Cards.

6. Who can perform accreditation of PIV Card Issuing Organizations?

Accreditation may be performed by a Designated Accreditation Authority (DAA) of a Federal agency who will assess the capabilities and reliability of its PCI(s) using NIST Special Publication (SP) 800-79 entitled ***"Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations".*** As stated in FIPS 201, Federal agencies may self-accredit their own PCIs, or use other accredited PCIs, to create identity credentials for their Federal employees and contractors. After additional experience is gained and resources are obtained, an independent accreditation process may be initiated to provide additional confidence that all PCIs are performing the needed services correctly and reliably.

7. Under whose authority and direction will accreditation be done?

Each agency is responsible for obtaining PIV Card issuing services and its Designated Accreditation Authority (DAA) is responsible for assuring that the organization uses the services of a PCI whose reliability has been accredited. NIST is responsible for developing guidelines for accrediting PCIs and is working closely with the Federal Identity Credentialing Committee (FICC) and the Office of Management and Budget to assure that appropriate guidance is available on a timely basis.

8. When must accreditation be performed?

Accreditation of the reliability of a PCI must be performed and completed as specified in FIPS 201. For PIV-I, accreditation of the reliability of the identity proofing and registration processes must be performed before issuing PIV credentials and registering Applicants. For PIV-II, accreditation of the reliability of the identity proofing, registration, PIV Card Issuing, and PIV Card lifecycle management processes of a PCI must be performed before any PIV Cards are issued. Accreditation should be performed following the planning, initiation, and implementation activities that establish a PCI. Certification will assure that the required attributes specified in SP 800-79 are assessed and found acceptable. Re-accreditation is needed whenever a significant change to the PIV Card issuing organization is made, the quality control monitoring activities detect any reduction of reliability, or three (3) years, whichever time period is least.

9. What services and operations are expected of a PCI?

The services and operations include:

1) Reviewing each request by an agency official for issuing a PIV Card;
2) Reviewing and vetting the identity source documents provided by the Applicant;
3) Assuring that the National Agency Checks, or their equivalent, authenticate and verify the identity claimed by the Applicant;
4) Entering the required personal Information in Identifiable Form (IIF) into the PIV System database for archival purposes as well as for the later rapid electronic verification of the identity when access is requested;
5) Maintaining a sufficient inventory supply of PIV Card stock;
6) Initializing a sufficient working supply of PIV Cards with application programs, access control interface software, and cryptographic algorithms;
7) Electronically acquiring digitized fingerprint and facial images from an Applicant to store on a personalized PIV card;
8) Generating and entering the cryptographic keys and personal authentication and authorization credentials of the Applicant on the PIV Card;
9) Producing (i.e., printing) a PIV Card with the required information for visual PIV;
10) Obtaining the necessary affirmation from an Applicant that a PIV Card has been received;
11) Providing information to an Applicant on how to use and protect a PIV Card;
12) Updating the PIV System database to allow the new PIV System user access to authorized resources when requested later;
13) Maintaining the PIV System and its database when PIV Cards are revoked, lost, stolen, replaced, etc.;
14) Ensuring the privacy of the personal IIF in the PIV System databases by controlling access, storage, dissemination, usage, and disposal;
15) Ensuring the secure and reliable operation of their part of the PIV System.

10. Will one organization provide PIV system design and integration services to ensure that all PIV system service providers can interoperate properly?

Each agency is responsible for obtaining PIV Card issuing services, either by establishing its own or by obtaining the needed services form other agencies or contractors. Each PCI must satisfy the requirements of FIPS 201 which includes interoperability. NIST is working on a PIV System design, implementation guidelines, conformance tests, product validation tests, and demonstrations to help PCIs implement the standard and to interoperate with each other. The Federal Identity Credentialing Committee is developing a Personal Identity Management handbook providing assistance for satisfying FIPS 201.

11. Will all agencies be required to provide equivalent interoperable PIV services?

The PIV System may be viewed as a single, integrated, interoperable system with a common set of objectives, policies, communication protocols, and application programs but with autonomous management of independent implementations, independently manufactured components, and evolving technology foundations. This is similar to the Internet with its common networking architecture, communication protocols, and interoperable application programs while supporting independent users operating within their own local environments. The PIV System is intended to verify the identity of a PIV Cardholder no matter who issues the Card from wherever the request for access is made.

12. Will additional value-added services be allowed on the PIV System?

Other services can coexist with those required for the PIV System in any current or future computer network. The PIV System should be viewed as a logical system rather than a physically separate system. Existing computer networks could easily support all the services and perform all the tasks required in the PIV System. Security of the PIV System and privacy of the Information in Identifiable Form (IIF) must be assured to satisfy FIPS 201 but privacy protection and security mechanisms should be place for other reasons. Access control systems are already used and only need to be converted to use the identity verified by the PIV System. The major impact on existing systems will be the requirement for interoperability of PIV components within the PIV System among all Federal agencies.

13. Will there be one organization identified as the security administrator of the PIV System?

A centralized security administrator of the PIV System is not expected. Each agency is responsible for its own networks, computer systems, information security, employee identity vetting, and access control systems. OMB will provide overall security policy guidance and NIST will provide security technology standards and supporting component validation testing services. Security of the automated systems that are part of the PIV System should be certified and accredited in accordance with NIST Special Publication 800-37.

14. Will there be one official responsible for the privacy of all the PIV system?

FIPS 201 states, “To ensure the privacy of Applicants, departments and agencies shall … assign an individual to the role of senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard. The individual serving in this role may not assume any other operational role in the PIV system.” Section 2.4 of FIPS 201 specifies additional requirements for protecting IIF. OMB provides guidance on privacy matters and provides assistance if questions about privacy arise.

15. Can security, privacy, and accreditation responsibilities be delegated to contractors?

Federal agencies can contract for services to assist them in security, privacy, and accreditation tasks but cannot delegate their authority or responsibilities in these areas to contractors. Each agency will remain responsible and accountable for the services and operations of the contractors. A contractor cannot be a DAA for a Federal organization.